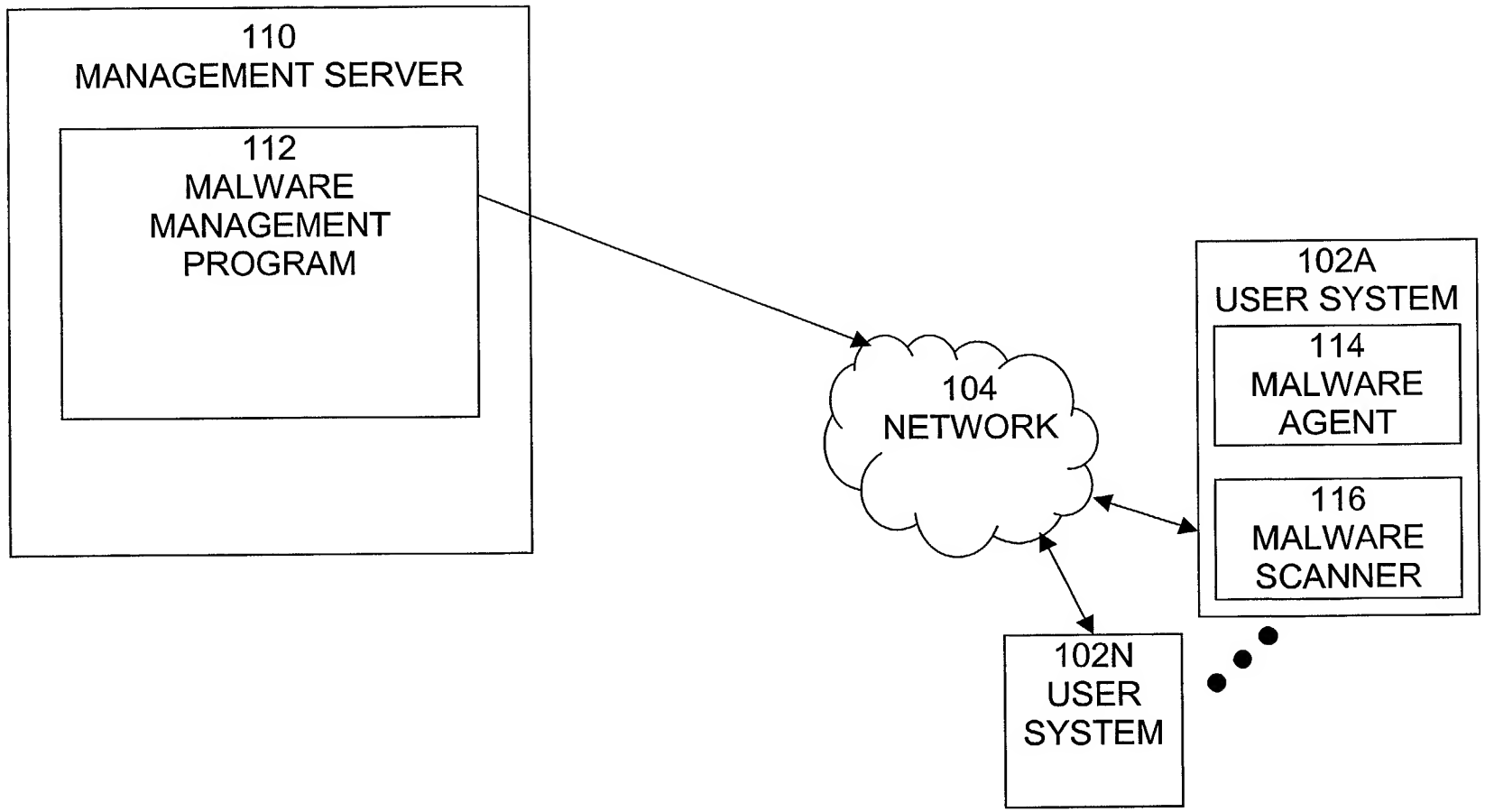
Fig. 1


110
MANAGEMENT SERVER
112
MALWARE
MANAGEMENT
PROGRAM
104
NETWORK
102A
USER SYSTEM
114
MALWARE
AGENT
116
MALWARE
SCANNER
102N
USER
SYSTEM

100

Fig. 2

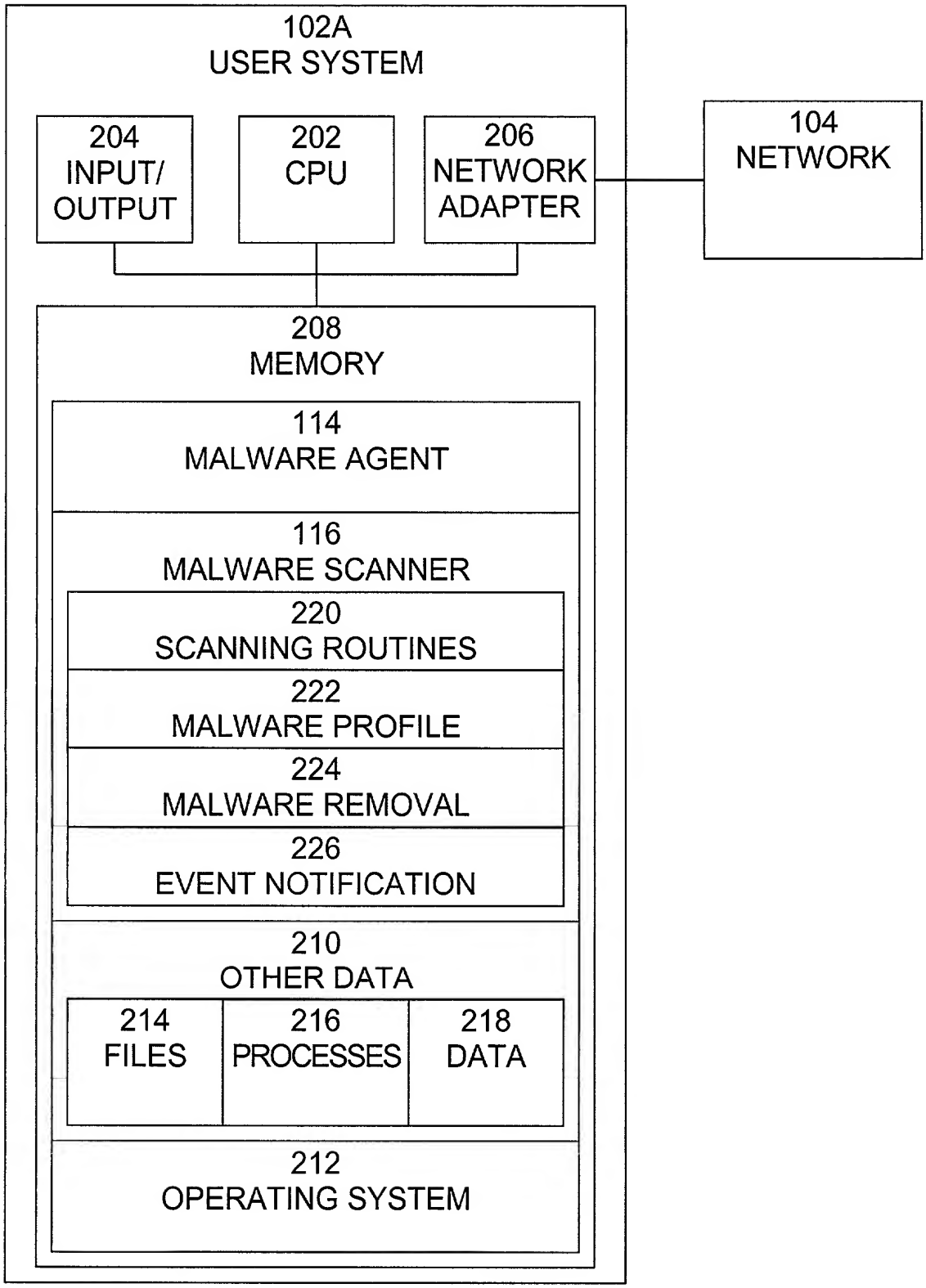

102A
USER SYSTEM
204
INPUT/
OUTPUT
202
CPU
206
NETWORK
ADAPTER
104
NETWORK
208
MEMORY
114
MALWARE AGENT
116
MALWARE SCANNER
220
SCANNING ROUTINES
222
MALWARE PROFILE
224
MALWARE REMOVAL
226
EVENT NOTIFICATION
210
OTHER DATA
214
FILES
216
PROCESSES
218
DATA
212
OPERATING SYSTEM

Fig. 3

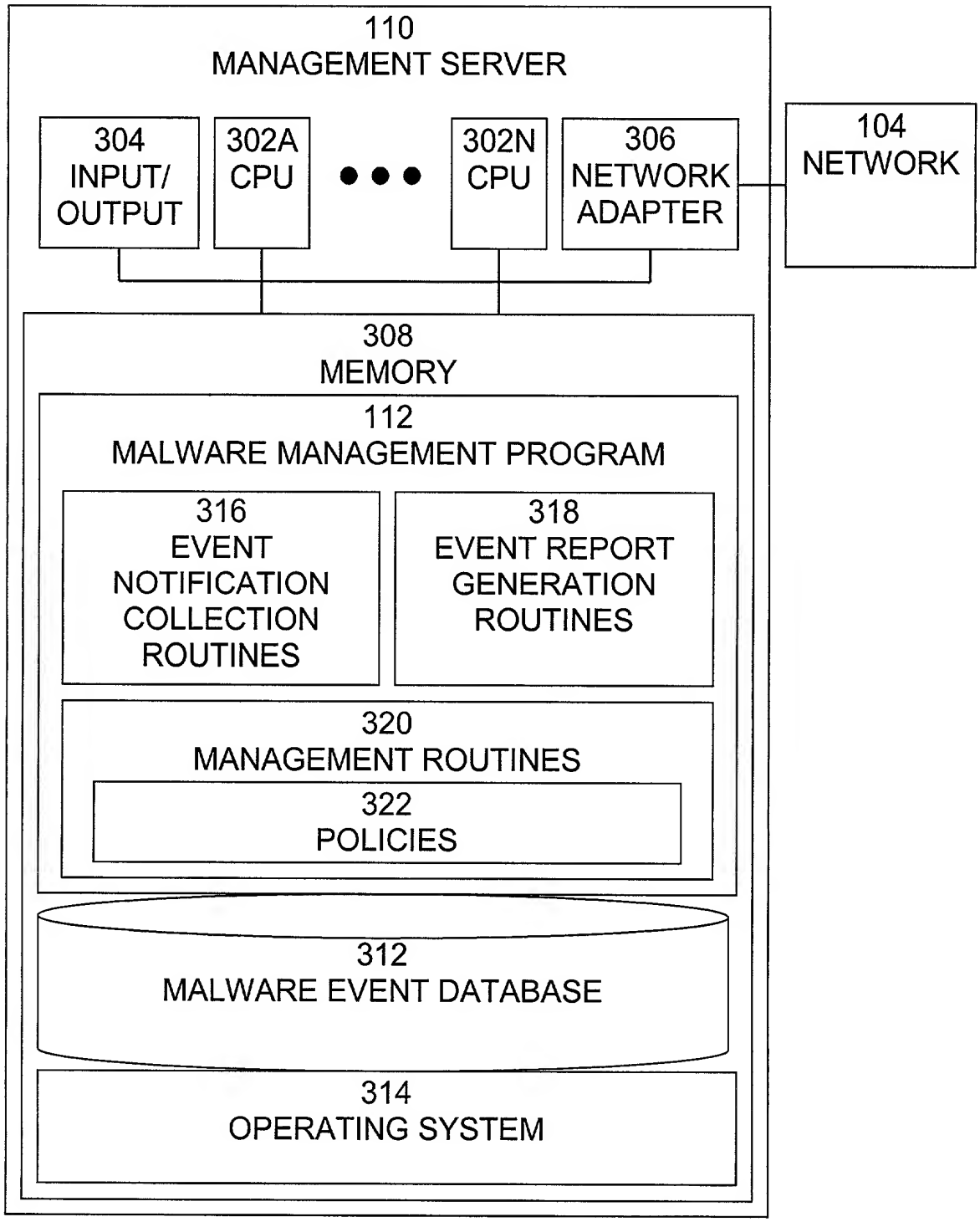

110
MANAGEMENT SERVER
304
INPUT/
OUTPUT
302A
CPU
302N
CPU
306
NETWORK
ADAPTER
104
NETWORK
308
MEMORY
112
MALWARE MANAGEMENT PROGRAM
316
EVENT
NOTIFICATION
COLLECTION
ROUTINES
318
EVENT REPORT
GENERATION
ROUTINES
320
MANAGEMENT ROUTINES
322
POLICIES
312
MALWARE EVENT DATABASE
314
OPERATING SYSTEM

Fig. 4

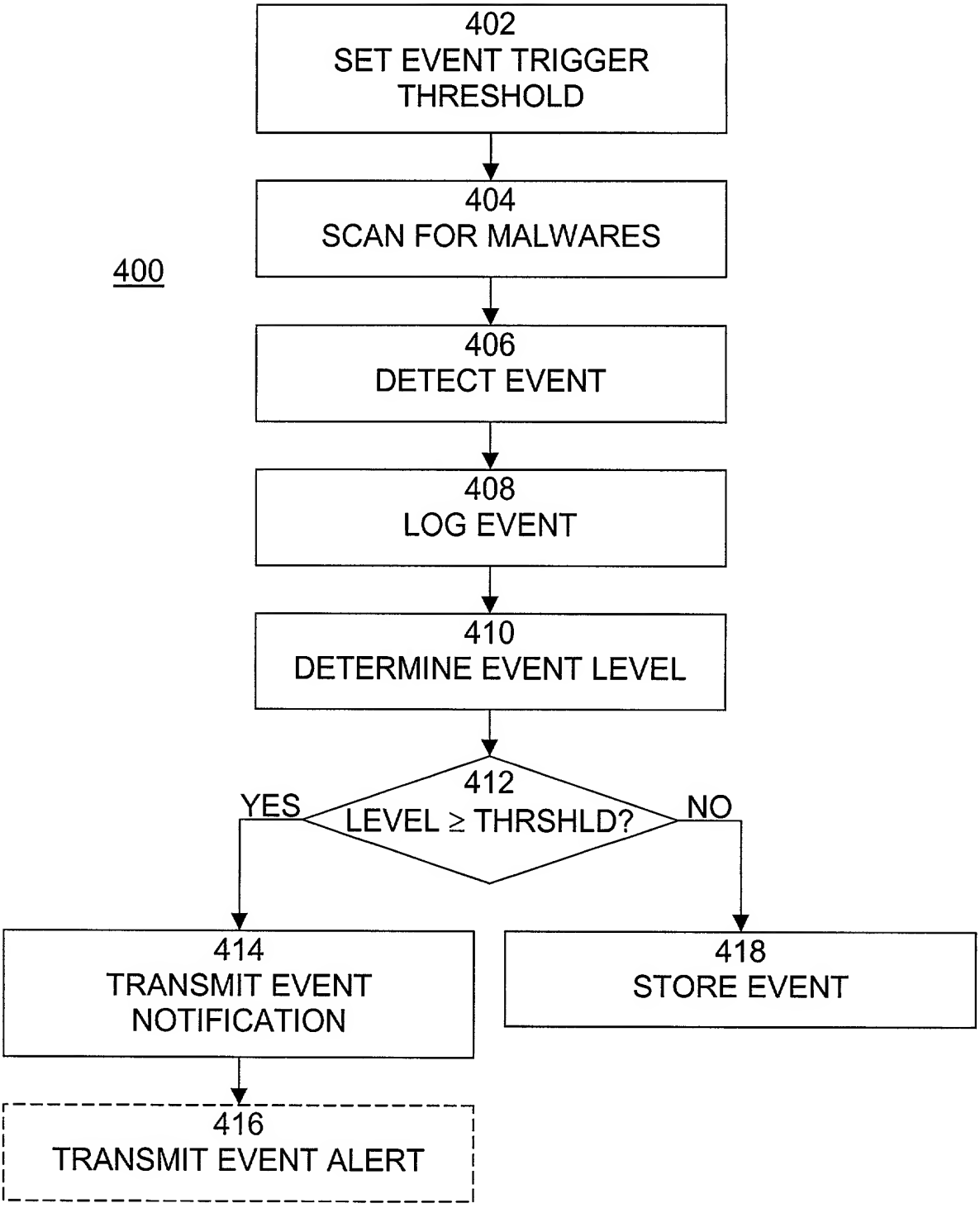
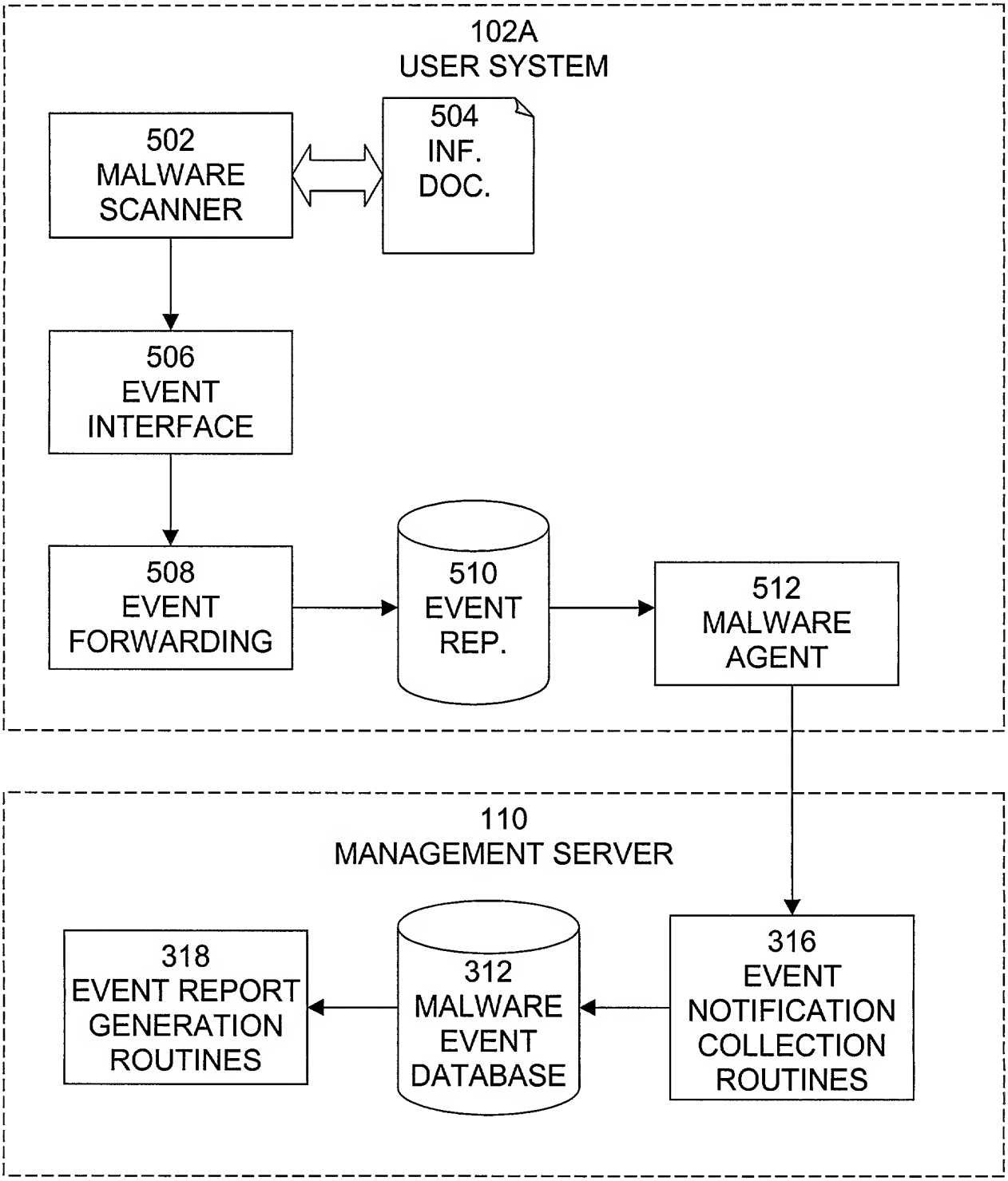

400
402
SET EVENT TRIGGER THRESHOLD
404
SCAN FOR MALWARES
406
DETECT EVENT
408
LOG EVENT
410
DETERMINE EVENT LEVEL
412
LEVEL ≥ THRSHLD?
YES
NO
414
TRANSMIT EVENT NOTIFICATION
416
TRANSMIT EVENT ALERT
418
STORE EVENT

Fig. 5


102A
USER SYSTEM
502
MALWARE
SCANNER
504
INF.
DOC.
506
EVENT
INTERFACE
508
EVENT
FORWARDING
510
EVENT
REP.
512
MALWARE
AGENT
110
MANAGEMENT SERVER
318
EVENT REPORT
GENERATION
ROUTINES
312
MALWARE
EVENT
DATABASE
316
EVENT
NOTIFICATION
COLLECTION
ROUTINES